

Regular balanced Cayley maps on $\text{PSL}(2, p)$

Haimiao Chen *

Beijing Technology and Business University, Beijing, China

Abstract

A *regular balanced Cayley map* (RBCM for short) on a finite group Γ is an embedding of a Cayley graph on Γ into a surface, with some special symmetric property. People have classified RBCM's for cyclic, dihedral, generalized quaternion, dicyclic, and semi-dihedral groups. In this paper we classify RBCM's on the group $\text{PSL}(2, p)$ for each prime number $p > 3$.

1 Introduction

Let Γ be a finite group and let Ω be a generating set not containing the identity and $\omega^{-1} \in \Omega$ whenever $\omega \in \Omega$. The *Cayley graph* $\text{Cay}(\Gamma, \Omega)$ is the graph having vertex set $V = \Gamma$ and arc set $\Gamma \times \Omega$, where (η, ω) means the arc from the vertex η to $\eta\omega$. If ρ is a cyclic permutation on Ω , then it gives a cyclic order to the set of arcs starting from η for each η , via $(\eta, \omega) \mapsto (\eta, \rho(\omega))$. This determines a unique cellular embedding of the Cayley graph $\text{Cay}(\Gamma, \Omega)$ into a closed oriented surface, where “cellular” means that each connected component of the complement of the embedded graph is homeomorphic to a disk. Such an embedding is called a *Cayley map* and is denoted by $\mathcal{CM}(\Gamma, \Omega, \rho)$.

An *isomorphism* between two Cayley maps is an isomorphism of the underlying graphs which is compatible with cyclic orders.

A Cayley map $\mathcal{CM}(\Gamma, \Omega, \rho)$ is called *regular* if its automorphism group acts transitively on the arc set, and called *balanced* if $\rho(\omega^{-1}) = \rho(\omega)^{-1}$ for all $\omega \in \Omega$. From now on we abbreviate “regular balanced Cayley map” to “RBCM”. The following proposition collects some well-known facts, for which one may refer to [10–12].

*Email: chenhm@math.pku.edu.cn. This work is supported by NSFC-11401014.

Proposition 1.1. (a) A Cayley map $\mathcal{CM}(\Gamma, \Omega, \rho)$ is a RBCM if and only if ρ extends to an isomorphism of Γ .

(b) For a RBCM $\mathcal{CM}(\Gamma, \Omega = \{\omega_i : 1 \leq i \leq m\}, \rho)$ with $\rho(\omega_i) = \omega_{i+1}$, all of the elements of Ω have the same order, and

(I) either $m = 2n$ and $\omega_{i+n} = \omega_i^{-1}$ for all i ,

(II) or all the ω_i 's are involutions, (i.e., have order 2).

A RBCM in the case (I) or (II) is said to be of type I or II, and denoted by I-RBCM or II-RBCM, respectively.

(c) If $\mathcal{CM}(\Gamma, \Omega, \rho)$ and $\mathcal{CM}(\Gamma', \Omega', \rho')$ are two RBCM's of the same type, then they are isomorphic if and only if there exists an isomorphism $f : \Gamma \rightarrow \Gamma'$ such that $f(\Omega) = \Omega'$ and $f \circ \rho = \rho' \circ f$.

A RBCM on a group Γ is not only a combinatorial object with good symmetry property, but also can be considered as an extra structure on Γ . So far, RBCM's have been classified for cyclic, dihedral, generalized quaternion, dicyclic, and semi-dihedral groups; see [7, 9, 12]. Recently, the first author [2] classified RBCM's for several subclasses of abelian p -groups.

In this paper, we classify RBCM's on $\text{PSL}(2, p)$ with $p > 3$ a prime number. This is the first time to obtain concrete results for a family of simple groups. Two key ingredients are involved in our idea: (i) each automorphism of $\text{PSL}(2, p)$ is the conjugation by a unique element of $\text{PGL}(2, p)$, and (ii) maximal subgroups of $\text{PSL}(2, p)$ are known, as recalled in Proposition 2.2. By Proposition 1.1, to classify $2n$ -valent I-RBCM's on $\text{PSL}(2, p)$, it suffices to find all pairs (σ, ω) with $\sigma \in \text{PGL}(2, p)$ and $\omega \in \text{PSL}(2, p)$ such that σ has order $2n$, $\sigma^n \omega \sigma^{-n} = \omega^{-1}$ and $\sigma^i \omega \sigma^{-i}, i = 1, \dots, n$ generate $\text{PSL}(2, p)$, (these conditions ensure that the conjugacy class of ω under σ has size $2n$). Note that the last condition is equivalent to that the subgroup generated by $\sigma^i \omega \sigma^{-i}, i = 1, \dots, n$ is not contained in any maximal subgroup of $\text{PSL}(2, p)$. The RBCM's determined by two pairs (σ, ω) and (σ', ω') are isomorphic if and only if there exists $\tau \in \text{PGL}(2, p)$ such that $\sigma' = \tau \sigma \tau^{-1}$ and $\omega' = \tau \omega \tau^{-1}$. The method for classifying II-RBCM's is similar.

The content is organized as follows. In Section 2 we recall some well-known facts about $\text{PSL}(2, p)$ and $\text{PGL}(2, p)$. In Section 3 and 4 we classify I-RBCM's and II-RBCM's on $\text{PSL}(2, p)$, respectively; in each section we separately deal with the cases $p = 5$ and $p > 5$, because $\text{PSL}(2, 5) = A_5$ plays a special role in subgroup structure of $\text{PSL}(2, p)$.

Notation 1.2. For a RBCM $\mathcal{CM}(\text{PSL}(2, p), \Omega, \rho)$, if $\Omega = \{\sigma^i \omega \sigma^{-i} : 1 \leq i \leq m\}$ with $\sigma \in \text{PGL}(2, p)$, then we denote $\mathcal{CM}(\text{PSL}(2, p), \Omega, \rho)$ by $\mathcal{CM}_\omega^\sigma$, with the understanding that the permutation ρ is given by $\sigma^i \omega \sigma^{-i} \mapsto \sigma^{i+1} \omega \sigma^{-(i+1)}$.

For a set X , denote its cardinality by $\#X$.

For an element μ of a group Γ , denote its order by $|\mu|$. Given a set of elements $\mu_1, \dots, \mu_\ell \in \Gamma$, denote the subgroup they generate by $\langle \mu_1, \dots, \mu_\ell \rangle$.

For two permutations ω and ψ , use $\omega\psi$ to mean “first do ω , then do ψ ”. For instance, $(12)(23) = (132)$.

Denote the 2×2 identity matrix by ε .

2 Preliminary

For a finite field \mathbb{F} , let \mathbb{F}^\times denote the multiplicative group of units. Consider \mathbb{F}_p as a subfield of \mathbb{F}_{p^2} . Fix a generator e of the cyclic group \mathbb{F}_p^\times and fix a square root $\sqrt{e} \in \mathbb{F}_{p^2}^\times$, then elements of \mathbb{F}_{p^2} are linear combinations $a + b\sqrt{e}$ with $a, b \in \mathbb{F}_p$. The *norm*

$$\begin{aligned} \mathcal{N} : \mathbb{F}_{p^2}^\times &\rightarrow \mathbb{F}_p^\times, \\ \mathcal{N}(a + b\sqrt{e}) &= a^2 - eb^2 = (a + b\sqrt{e})^{p+1}, \end{aligned}$$

is a surjective homomorphism (see Problem 1 on Page 87 of [8]).

Fix a generator $w_1 + w_2\sqrt{e}$ of the cyclic group $\mathbb{F}_{p^2}^\times$ and let $w = w_1/w_2$, then $w^2 - e$ has no square root in \mathbb{F}_p .

Let

$$\alpha = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} w & e \\ 1 & w \end{pmatrix}. \quad (1)$$

It is well-known that (one may refer to [4], Page 68) each element of $\text{PGL}(2, p)$ is conjugate to α^k for some k , or β , or γ^ℓ for some ℓ . Furthermore, $\alpha^{k'}$ is conjugate to α^k if and only if $k' = \pm k$, and $\gamma^{\ell'}$ is conjugate to γ^ℓ if and only if $\ell' = \pm \ell$.

The following enables us to conveniently deal with the orders of elements of $\text{PSL}(2, p)$, and can be proved by repeatedly applying Hamilton-Cayley Theorem $\tilde{\eta}^2 = t\tilde{\eta} - \varepsilon$.

Proposition 2.1. *Let $\tilde{\eta} \in \text{SL}(2, p)$ with $\text{tr}(\tilde{\eta}) = t$, and let $\eta \in \text{PSL}(2, p)$ denote the image of $\tilde{\eta}$ under the quotient homomorphism $\text{SL}(2, p) \rightarrow \text{PSL}(2, p)$.*

- (a) $|\eta| = 2$ if and only if $t = 0$,
- (b) $|\eta| = 3$ if and only if $t^2 = 1$,
- (c) $|\eta| = 4$ if and only if $t^2 = 2$,

- (d) $|\eta| = 5$ if and only if $(t^2 - 1)^2 = t^2$.

The following result is quoted from Proposition 2.1 of [5]; also see [3].

Proposition 2.2. *Suppose $p \geq 5$. Then each maximal subgroup of $\text{PSL}(2, p)$ has one of the following forms:*

- (i) *the stabilizer of a point on the projective line $\mathbb{P}^1(\mathbb{F}_p)$;*
- (ii) *$D_{p \pm 1}$, the dihedral group of order $p \pm 1$;*
- (iii) *A_4 , S_4 or A_5 .*

Remark 2.3. A subgroup of form (i) is the same as one whose elements have a common eigenvector.

A subgroup of form (ii) means one isomorphic to $D_{p \pm 1}$, and similarly for (iii). Subgroups in (ii) or (iii) do not always exist, and even when they exist, they may not be maximal.

Finally, recall some facts about S_4 , $\text{PSL}(2, 5) = A_5$ and $\text{PGL}(2, 5) = S_5$:

Proposition 2.4. (a) *Nontrivial conjugacy classes of S_5 are listed below (using $[\mu]$ to denote the conjugacy class containing μ):*

$$[(12345)], \quad [(123)], \quad [(12)(34)], \quad [(12)(345)], \quad [(1234)], \quad [(12)],$$

where the first three classes are contained in A_5 .

- (b) *S_4 has a presentation $\langle X, Y | X^2, Y^3, (XY)^4 \rangle$, so any group generated by two elements μ, η with $|\mu| = 2$, $|\eta| = 3$ and $|\mu\eta| = 4$ is a quotient of S_4 .*
- (c) *A_5 has a presentation $\langle X, Y | X^2, Y^3, (XY)^5 \rangle$, so any nontrivial group generated by two elements μ, η with $|\mu| = 2$, $|\eta| = 3$ and $|\mu\eta| = 5$ is isomorphic to A_5 .*
- (d) *Each non-abelian proper subgroup of A_5 is isomorphic to D_6 , D_{10} or A_4 .*

We explain (d). Let $\Gamma \leq A_5$ be a non-abelian proper subgroup, then $\#\Gamma \in \{6, 10, 12, 15, 20\}$. Clearly Γ is dihedral if $\#\Gamma \in \{6, 10\}$. By [1] Theorem 7.8.1 which classifies groups of order 12, $\Gamma = A_4$ if $\#\Gamma = 12$. By [1] Theorem 7.7.7 (a), each group of order 15 is cyclic, so $\#\Gamma$ never equals 15. Finally, if $\#\Gamma = 20$, then by Sylow's Theorem, Γ has exactly one subgroup of order 5, so all the other 15 elements are involutions, which are exactly all the 15 involutions in A_5 , but the product of $(12)(34)$ and $(12)(35)$ is (345) , whose order cannot divide 20.

3 Type I regular balanced Cayley maps

3.1 I-RBCM's on $\text{PSL}(2, 5) = A_5$

Suppose $\mathcal{CM}_\omega^\sigma$ is a I-RBCM on $\text{PSL}(2, 5) = A_5$, with $\omega \in A_5$, $|\omega| > 2$, $\sigma \in S_5$, $|\sigma| = 2n$. Clearly $2 < 2n \leq 6$, hence $n = 2$ or $n = 3$. We may assume that ω is one of representatives of conjugacy classes as in Proposition 2.4 (a), namely, $\omega = (123)$ or $\omega = (12345)$. Denote $\omega_i = \sigma^i \omega \sigma^{-i}$, $1 \leq i \leq 2n$.

There are four possibilities.

- If $n = 2$ and $\omega = (123)$, then it follows from $\omega_2 = \omega^{-1}$ that $\sigma = (k4\ell5)$ with $\{k, \ell\} \subset \{1, 2, 3\}$. We may find $\tau \in \{(1), \omega, \omega^2\}$ such that $\tau\sigma\tau^{-1} = (1425)$ and $\mathcal{CM}_\omega^{\tau\sigma\tau^{-1}} \cong \mathcal{CM}_\omega^\sigma$. Just assume $\sigma = (1425)$. Now $\omega_1 = (543)$, $\omega\omega_1\omega_1^{-1} = (14)(23)$ has order 2, and $(\omega\omega_1\omega_1^{-1})\omega_1 = \omega\omega_1\omega = (13254)$ has order 5, thus $\langle \omega\omega_1\omega_1^{-1}, \omega_1 \rangle = A_5$ and also $\langle \omega_1, \omega_2 \rangle = A_5$.
- If $n = 2$ and $\omega = (12345)$, then by replacing σ by $\omega^k \sigma \omega^{-k}$ for some k if necessary, we may assume σ fixes the letter 5. Hence $\sigma = (1243)$ or $\sigma = (1342)$, due to the condition $\omega_2 = \omega^{-1}$. If $\sigma = (1243)$, then $\omega_1 = (31425) = \omega^{-2}$; if $\sigma = (1342)$, then $\omega_1 = (24135) = \omega^2$. In neither case $\langle \omega, \sigma\omega\sigma^{-1} \rangle = A_5$, as A_5 is not cyclic.
- If $n = 3$ and $\omega = (123)$, then $\sigma = (k_1 k_2)(\ell_1 \ell_2 \ell_3)$ with $\{k_1, k_2\} \subset \{1, 2, 3\}$ due to $\omega_3 = \omega^{-1}$. By replacing σ by $\omega^k \sigma \omega^{-k}$ for some k if necessary, we may assume $\sigma = (12)(345)$, hence $\omega_1 = (215)$, $\omega_2 = (124)$. Now $\omega\omega_1^{-1} = (15)(23)$, $(\omega\omega_1^{-1})\omega_2 = (15234)$, so $\langle \omega\omega_1^{-1}, \omega_2 \rangle = A_5$ and also $\langle \omega_1, \omega_2, \omega_3 \rangle = A_5$.
- If $n = 3$ and $\omega = (12345)$, then it is impossible that $\sigma^3 \omega \sigma^{-3} = \omega^{-1}$, since σ^3 is a transposition.

Theorem 3.1. *Each 4-valent I-RBCM on A_5 is isomorphic to $\mathcal{CM}_{(123)}^{(1425)}$, each 6-valent type I RBCM on A_5 is isomorphic to $\mathcal{CM}_{(123)}^{(12)(345)}$, and there does not exist a $2n$ -valent I-RBCM for $n > 3$.*

3.2 I-RBCM's on $\text{PSL}(2, p)$ for $p > 5$

Suppose $\mathcal{CM}_\omega^\sigma$ is a $2n$ -valent I-RBCM with $|\sigma| = 2n \geq 4$, noting that $\text{PSL}(2, p)$ is not cyclic. Now that σ is conjugate to α^k or γ^ℓ , we may just assume $\sigma = \alpha^k$ with $1 \leq k \leq (p-1)/2$, or $\sigma = \gamma^\ell$ with $1 \leq \ell \leq (p+1)/2$.

Setting

$$\tau = \begin{cases} \varepsilon, & \text{if } \sigma = \alpha^k, \\ \begin{pmatrix} \sqrt{e} & -e \\ \sqrt{e} & e \end{pmatrix}, & \text{if } \sigma = \gamma^\ell, \end{cases} \quad (2)$$

one has

$$\tau\sigma\tau^{-1} = \begin{pmatrix} s & 0 \\ 0 & 1/s \end{pmatrix} \in \text{PGL}(2, p^2), \quad \text{with } s = \begin{cases} (\sqrt{e})^k, & \text{if } \sigma = \alpha^k, \\ \left(\frac{w-\sqrt{e}}{\sqrt{w^2-e}}\right)^{-\ell}, & \text{if } \sigma = \gamma^\ell; \end{cases} \quad (3)$$

note that s has order $4n$ as an element of $\mathbb{F}_{p^2}^\times$, hence $s^{2n} = -1$.

Suppose

$$\tau\omega\tau^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}(2, p^2), \quad \text{with } a^2 - bc = 1. \quad (4)$$

The condition $\sigma^n\omega\sigma^{-n} = \omega^{-1}$ is equivalent to $\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, implying $a = d$.

Lemma 3.2. *The elements $\sigma^i\omega\sigma^{-i}$, $i = 1, \dots, n$ generate $\text{PSL}(2, p)$ if and only if $abc \neq 0$ and $2a^2 \neq 1$ when $n = 2$.*

Proof. Let $\Gamma = \langle \psi_1, \dots, \psi_n \rangle$ with $\psi_i = \tau\sigma^i\omega\sigma^{-i}\tau^{-1}$. The task is to show $\tau^{-1}\Gamma\tau = \text{PSL}(2, p)$. We have

$$\psi_i = \begin{pmatrix} a & s^{2i}b \\ s^{-2i}c & a \end{pmatrix}, \quad \psi_i\psi_j = \begin{pmatrix} a^2 + s^{2(i-j)}bc & (s^{2i} + s^{2j})ab \\ (s^{-2i} + s^{-2j})ac & a^2 + s^{2(j-i)}bc \end{pmatrix}. \quad (5)$$

If $a = 0$, then ψ_i is counter-diagonal, so each element of Γ is either diagonal or counter-diagonal, hence

$$\#\Gamma \leq 2(p^2 - 1) < p(p^2 - 1)/2 = \#\text{PSL}(2, p).$$

If $bc = 0$, then ψ_i is unipotent, hence also $\#\Gamma < \#\text{PSL}(2, p)$.

Thus a necessary condition for $\tau^{-1}\Gamma\tau = \text{PSL}(2, p)$ is $abc \neq 0$. We show that this is also sufficient except for the case when $n = 2$ and $2a^2 = 1$.

Suppose $abc \neq 0$. Then $|\psi_i| > 2$, as $\text{tr}(\psi_i) = 2a \neq 0$.

(a) If $\Gamma \leq D_{2m}$, then $\psi_i \in \mathbb{Z}/m\mathbb{Z}$, but by Eq.(5) Γ is not abelian.

(b) If Γ is contained in a subgroup of form (i) in Proposition 2.2, then ψ_1 and ψ_2 have a common eigenvector $(x, y)^t \in \mathbb{F}_{p^2}^2$, hence both (x, y) and $(sx, y)^t$ are eigenvectors of ψ_1 ; this implies $x = 0$ or $y = 0$, which contradicts the assumption that $bc \neq 0$.

(c) If $\Gamma \leq S_4$, then $\Gamma = A_4$ or S_4 according to (a). It is well-known that each automorphism of A_4 or S_4 is the conjugation by some element in S_4 , whose order belongs to $\{2, 3, 4\}$, hence $n = 2$, $s^4 = -1$ and $\text{tr}(\psi_1\psi_2) = 2a^2$, using Eq.(5). If $|\psi_i| = 3$, then $\Gamma = A_4$, and $4a^2 = (\text{tr}(\psi_1))^2 = 1$, so $\text{tr}(\psi_1\psi_2) = 1/2$, implying $|\psi_1\psi_2| \neq 2, 3$, but this contradicts $\psi_1\psi_2 \in A_4$. Thus $|\psi_i| = 4$, and $2a^2 - 1 = \text{tr}(\psi_2^2) = 0$, i.e., $2a^2 = 1$.

Conversely, if $n = 2$ and $2a^2 = 1$, then (denoting $\tau\sigma\tau^{-1}$ by ς)

$$(\text{tr}(\varsigma\psi_4))^2 = (s + s^{-1})^2 a^2 = 1, \quad \text{tr}(\varsigma^2\psi_4) = (s^2 + s^{-2})a^2 = 0,$$

hence $|\varsigma\psi_4| = 3$ and $|\psi_4^{-1}\varsigma^{-2}| = |\varsigma^2\psi_4| = 2$; this together with $|(\psi_4^{-1}\varsigma^{-2})(\varsigma\psi_4)| = |\varsigma| = 4$ implies that $\langle \varsigma, \psi_4 \rangle = \langle \psi_4^{-1}\varsigma^{-2}, \varsigma\omega \rangle$ is a quotient of S_4 . Thus $\#\Gamma \leq 24$.

(d) If $\Gamma \leq A_5$, then $\Gamma = A_5$ by (a) and Proposition 2.4 (d). By Theorem 3.1, there are two possibilities; in both cases $|\psi_i| = 3$ hence $4a^2 = 1$.

- (i) $n = 2$ (so that $s^4 = -1$), then $\text{tr}(\psi_1\psi_2) = 2a^2 \neq 0, \pm 1$ and is not a root of $(t^2 - 1)^2 = t^2$, hence $|\psi_1\psi_2| \notin \{2, 3, 5\}$, contradicting $\psi_1\psi_2 \in A_5$.
- (ii) $n = 3$ (so that $s^4 - s^2 + 1 = 0$), then there exists an isomorphism $A_5 \cong \Gamma$ sending (215) to ψ_1 and (124) to ψ_2 , hence it sends $(154) = (215)(124)$ to $\psi_1\psi_2$. But $\text{tr}(\psi_1\psi_2) = 3a^2 - 1 = -1/4 \neq \pm 1$, a contradiction.

□

If $\sigma = \alpha^k$, then $2n \mid p-1$ and $k = (p-1)u/2n$ for some u with $(u, 2n) = 1$, $1 \leq u < n$. Now $\varphi := \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ commutes with α^k and

$$\varphi\omega\varphi^{-1} = \begin{pmatrix} a & 1 \\ a^2 - 1 & a \end{pmatrix} =: \omega(i, a), \quad (6)$$

thus $\mathcal{CM}_{\omega}^{\alpha^k} \cong \mathcal{CM}_{\omega(i, a)}^{\alpha^k}$. Furthermore, for $a \neq a'$, $\omega(i, a)$ is not conjugate to $\omega(i, a')$, as $\text{tr}(\omega(i, a)) \neq \text{tr}(\omega(i, a'))$, so $\mathcal{CM}_{\omega(i, a)}^{\alpha^k} \not\cong \mathcal{CM}_{\omega(i, a')}^{\alpha^k}$.

If $\sigma = \gamma^\ell$, then $2n \mid p+1$ and $\ell = (p+1)v/2n$ for some v with $(v, 2n) = 1$, $1 \leq v < n$. Note that, if $n = 2$, then $2a^2$ never equals 1 since the Legendre

symbol $(2/p) = -1$ by Theorem 1 (b) on Page 53 of [6]. By Eq.(2) and (4),

$$\omega = \begin{pmatrix} a + (b+c)/2 & \sqrt{e}(b-c)/2 \\ (c-b)/2\sqrt{e} & a - (b+c)/2 \end{pmatrix} = \begin{pmatrix} x & -ez \\ z & 2a-x \end{pmatrix} \in \text{PSL}(2, p), \quad (7)$$

where $x = a + (b+c)/2$ and $z = (c-b)/2\sqrt{e}$ are elements of \mathbb{F}_p , hence

$$(x-a)^2 - ez^2 = bc = a^2 - 1, \quad (8)$$

i.e., $\mathcal{N}(x-a+z\sqrt{e}) = a^2 - 1$. When a is fixed, this equation has $p+1$ solutions, since the homomorphism $\mathcal{N} : \mathbb{F}_{p^2}^\times \rightarrow \mathbb{F}_p^\times$ is surjective. Choose and fix a solution $(x_{i,a}, z_{i,a})$, and put

$$\tilde{\omega}(i, a) = \begin{pmatrix} x_{i,a} & -ez_{i,a} \\ z_{i,a} & 2a - x_{i,a} \end{pmatrix}. \quad (9)$$

Noticing

$$\tau\gamma\tau^{-1} = \begin{pmatrix} w - \sqrt{e} & 0 \\ 0 & w + \sqrt{e} \end{pmatrix}, \quad \text{and } \tau\tilde{\omega}(i, a)\tau^{-1} = \begin{pmatrix} a & b' \\ c' & -a \end{pmatrix}$$

for some b', c' with $b'c' = a^2 - 1$, we easily see that the $p+1$ elements

$$\gamma^h \tilde{\omega}(i, a) \gamma^{-h}, \quad h = 1, \dots, p+1$$

are distinct from each other. Thus for the present ω , there exist (a unique) $h \in \{1, \dots, p+1\}$ such that $\gamma^h \tilde{\omega}(i, a) \gamma^{-h} = \omega$, and hence $\mathcal{CM}_\omega^{\gamma^\ell} \cong \mathcal{CM}_{\tilde{\omega}(i,a)}^{\gamma^\ell}$.

Theorem 3.3. *Suppose \mathcal{M} is a $2n$ -valent I-RBCM on $\text{PSL}(2, p)$ with $p > 5$, then $2n \mid p-1$ or $2n \mid p+1$.*

- (i) *If $2n \mid p-1$, then $\mathcal{M} \cong \mathcal{CM}_{\omega(i,a)}^{\alpha^{(p-1)u/2n}}$ for a unique pair (a, u) such that $a \notin \{\pm 1, 0\}$, $(u, 2n) = 1$, $1 \leq u < n$, and moreover, $2a^2 \neq 1$ if $n = 2$.*
- (ii) *If $2n \mid p+1$, then $\mathcal{M} \cong \mathcal{CM}_{\tilde{\omega}(i,a)}^{\gamma^{(p+1)v/2n}}$ for a unique pair (a, v) such that $a \notin \{\pm 1, 0\}$, $(v, 2n) = 1$ and $1 \leq v < n$.*

4 Type II regular balanced Cayley maps

4.1 II-RBCM's on $\text{PSL}(2, 5) = A_5$

Suppose $\mathcal{CM}_\omega^\sigma$ is an n -valent II-RBCM on $\text{PSL}(2, 5) = A_5$, with $\omega \in A_5$, $|\omega| = 2$, and $\sigma \in S_5$, $|\sigma| = n \leq 6$. Since a nonabelian group generated by

two involutions must be dihedral, we have $n > 2$. Also note that the action of the conjugation by σ on the set of involutions of A_5 has at most one fixed element, hence $n \mid 15$ or $n \mid 14$ which implies $n = 3$ or $n = 5$.

Denote $\omega_i = \sigma^i \omega \sigma^{-i}$, $i = 1, \dots, n$, and denote $\Gamma = \langle \omega_1, \dots, \omega_n \rangle$.

If $n = 3$, we may assume $\sigma = (123)$ and ω fixes the letter 1. The condition $\langle \omega_1, \omega_2, \omega_3 \rangle = A_5$ requires $\omega \in \{(24)(35), (25)(34)\}$. The conjugation by (45) fixes σ and takes $(25)(34)$ to $(24)(35)$, so let us just assume $\omega = (24)(35)$. Then $\omega_1 = (14)(25)$, $\omega_2 = (15)(34)$, $\omega_1 \omega_2 \omega_1 \omega_3 = (153)$, $\omega_1(\omega_1 \omega_2 \omega_1 \omega_3) = \omega_2 \omega_1 \omega_3 = (14523)$, thus $\langle \omega_1, \omega_1 \omega_2 \omega_1 \omega_3 \rangle = A_5$, and also $\Gamma = A_5$.

If $n = 5$, we may assume $\sigma = (12345)$. There are three possibilities.

- (i) If $\omega_5 = (12)(34)$, then $\omega_1 = (15)(23)$, $\omega_2 = (12)(45)$, $\omega_3 = (15)(34)$, $\omega_4 = (23)(45)$, so $\omega_3 \omega_5 = (152)$, $\omega_5 \omega_4 = (13542)$, $\omega_5 \omega_4 \omega_5 \omega_3 = (13)(45)$, hence $\langle \omega_5 \omega_4 \omega_5 \omega_3, \omega_3 \omega_5 \rangle = A_5$ and also $\Gamma = A_5$.
- (ii) If $\omega_5 = (13)(24)$, then $\omega_1 = (13)(25)$, $\omega_2 = (14)(25)$, $\omega_3 = (14)(35)$, $\omega_4 = (24)(35)$, so $\omega_4 \omega_5 = (135)$, $\omega_5 \omega_2 = (13452)$, $\omega_5 \omega_2 \omega_5 \omega_4 = (25)(34)$, hence $\langle \omega_5 \omega_2 \omega_5 \omega_4, \omega_4 \omega_5 \rangle = A_5$ and also $\Gamma = A_5$.
- (iii) If $\omega_5 = (14)(23)$, then $\omega_1 = (12)(35)$, $\omega_2 = (15)(24)$, $\omega_3 = (13)(45)$, $\omega_4 = (25)(34)$, so $\omega_4 \omega_5 = (14253)$. One can check that $\omega_i = \omega_5(\omega_4 \omega_5)^i$, $i = 1, \dots, 5$, hence $\Gamma = \langle \omega_4, \omega_5 \rangle \cong D_{10}$, which is impossible.

Theorem 4.1. *Each 3-valent II-RBCM on A_5 is isomorphic to $\mathcal{CM}_{(24)(35)}^{(123)}$, each 5-valent II-RBCM on A_5 is isomorphic to $\mathcal{CM}_{(12)(34)}^{(12345)}$ or $\mathcal{CM}_{(13)(24)}^{(12345)}$, and there does not exist an n -valent II-RBCM on A_5 for $n \neq 3, 5$.*

4.2 II-RBCM's on $\text{PSL}(2, p)$ for $p > 5$

Let $\mathcal{CM}_\omega^\sigma$ be an n -valent II-RBCM on $\text{PSL}(2, p)$, with $|\omega| = 2$ and $|\sigma| = n > 2$ (as $\text{PSL}(2, p)$ is not dihedral). We may assume σ is equal to α^k , β or γ^ℓ . Suppose

$$\omega = \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \quad \text{with } x^2 + yz = -1. \quad (10)$$

If $n = p$, then $\sigma = \beta$, and

$$\beta^i \omega \beta^{-i} = \begin{pmatrix} x + iz & y - 2ix - i^2 z \\ z & -x - iz \end{pmatrix}, \quad 1 \leq i \leq p. \quad (11)$$

Lemma 4.2. *The elements $\beta^i \omega \beta^{-i}$, $i = 1, \dots, p$ generate $\text{PSL}(2, p)$ if and only if $z \neq 0$.*

Proof. Let $\Gamma = \langle \omega_1, \dots, \omega_p \rangle$ with $\omega_i = \beta^i \omega \beta^{-i}$. If $z = 0$, then each ω_i is upper-triangular, and so is each element of Γ , hence $\Gamma \neq \text{PSL}(2, p)$.

Suppose $z \neq 0$, we shall prove that $\Gamma = \text{PSL}(2, p)$.

Firstly, Γ is not contained in the stabilizer of any point of $\mathbb{P}^1(\mathbb{F}_p)$: if $\xi \in \mathbb{F}_p^2$ is a common eigenvector of ω_1 and ω_2 , then ξ and $\beta\xi$ are both eigenvectors of ω_1 , hence ξ and $\beta\xi$ are linearly dependent, which is impossible when $z \neq 0$.

Secondly, we show that Γ is not contained in any other maximal subgroup, by counting involutions. For a group Δ , let $I(\Delta)$ denote the set of involutions of Δ . It is obvious that $\beta^i \phi \beta^{-i} \neq \phi$ for any $\phi \in \text{PSL}(2, p)$ unless ϕ is upper-unitriangular, in which case $\phi \notin I(\Gamma)$, so $\langle \beta \rangle$ acts freely on $I(\Gamma)$ by conjugation. Thus

$$(\star) \quad p \mid \#I(\Gamma) \quad \text{and} \quad \#I(\Gamma) \geq p.$$

- It is impossible that $\Gamma \leq D_{p-1}$, since $\#I(D_{p-1}) = p - 1 < p$.

If $\Gamma \leq D_{p+1}$, then $\Gamma = D_{p+1}$ since any p involutions generate D_{p+1} ; but $\#I(D_{p+1}) = p + 1$ is not a multiple of p , contradicting (\star) .

- It is impossible that $\Gamma \leq A_4$, since $\#I(A_4) = 3 < p$.
- If $\Gamma \leq S_4$, then $\#I(\Gamma) = p = 7$ since $\#I(S_4) = 9$, but no subgroup of S_4 contains exactly 7 involutions.
- If $\Gamma \leq A_5$, then $\#I(\Gamma) = p \in \{7, 11, 13\}$ since $\#I(A_5) = 15$, but A_5 does not have such a subgroup Γ , as can be checked.

□

Let m be an integer whose residue class modulo p is $-x/z$, then

$$\beta^m \omega \beta^{-m} = \begin{pmatrix} 0 & -1/z \\ z & 0 \end{pmatrix} =: \varpi(z), \quad (12)$$

hence $\mathcal{CM}_\omega^\beta \cong \mathcal{CM}_{\varpi(z)}^\beta$. Furthermore, for $z \neq z'$, there does not exist τ with $\tau \beta \tau^{-1} = \beta$ and $\tau \varpi(z) \tau^{-1} = \varpi(z')$, so $\mathcal{CM}_{\varpi(z)}^\beta \not\cong \mathcal{CM}_{\varpi(z')}^\beta$.

If $n \neq p$, then take τ as in Eq.(2), so that

$$\varsigma := \tau \sigma \tau^{-1} = \begin{pmatrix} s & 0 \\ 0 & 1/s \end{pmatrix} \in \text{PGL}(2, p^2)$$

with s given by Eq.(3). Suppose

$$\tau\omega\tau^{-1} = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \text{PSL}(2, p^2). \quad (13)$$

Lemma 4.3. *The elements $\sigma^i\omega\sigma^{-i}, i = 1, \dots, n$ generate $\text{PSL}(2, p)$ if and only if $abc \neq 0$ and (i) $3a^2 \neq -1, -2$ and $9a^4 + 9a^2 + 1 \neq 0$ if $n = 3$, (ii) $5a^4 + 5a^2 + 1 \neq 0$ if $n = 5$.*

Proof. Let $\Gamma = \langle \psi_1, \dots, \psi_n \rangle$ with $\psi_i = \varsigma^i(\tau\omega\tau^{-1})\varsigma^{-i}$. We have

$$\psi_i = \begin{pmatrix} a & s^{2i}b \\ s^{-2i}c & -a \end{pmatrix}, \quad \psi_i\psi_j = \begin{pmatrix} a^2 + s^{2(i-j)}bc & (s^{2j} - s^{2i})ab \\ (s^{-2i} - s^{-2j})ac & a^2 + s^{2(j-i)}bc \end{pmatrix}. \quad (14)$$

It can be verified that $\psi_i, 1 \leq i \leq n$ have a common eigenvector if and only if $abc = 0$, so a necessary condition for $\tau^{-1}\Gamma\tau = \text{PSL}(2, p)$ is $abc \neq 0$ which we assume below.

(a) If $\Gamma \leq D_{2m}$ for some m , then $\psi_n\psi_1\psi_2$ is an involution, hence

$$0 = \text{tr}(\psi_n\psi_1\psi_2) = (2(s^{-2} - s^2) + s^4 - s^{-4})abc.$$

But this is impossible since $s^2 \neq \pm 1$. In particular, $\Gamma \not\leq D_{p\pm 1}$.

(b) If $\Gamma \leq A_4$, then since A_4 has exactly 3 involutions which commute with each other, we have $n = 3$ and $\psi_3\psi_1 = \psi_2$, hence $s^4 + s^2 + 1 = 0$ and

$$\begin{pmatrix} a^2 + s^4bc & (s^2 - 1)ab \\ (1 - s^4)ac & a^2 + s^2bc \end{pmatrix} = \begin{pmatrix} a & s^4b \\ s^2c & -a \end{pmatrix} \in \text{PSL}(2, p^2).$$

This is equivalent to $3a^2 = -1$, as can be verified.

(c) If $\Gamma \leq S_4$ but $\Gamma \not\leq A_4$, then $\Gamma = S_4$ since any other subgroup of S_4 is dihedral, which cannot contain Γ by (a). Recall that each automorphism of S_4 is the conjugation by some $\eta \in S_4$. Suppose the element of Γ corresponding to η is ϑ , then for each i , $\vartheta\psi_i\vartheta^{-1} = \psi_{i+1} = \varsigma\psi_i\varsigma^{-1}$, hence $\varsigma^{-1}\vartheta$ commutes with ψ_i ; this implies that $\vartheta = \varsigma$ since the ψ_i 's have no common eigenvector. Thus $\varsigma \in \Gamma$.

Below, we write elements of Γ and also ς as matrices and permutations simultaneously. Clearly each ψ_i is a transposition; just assume $\psi_n = (12)$. There are two possibilities.

(i) If $n = 3$, then ς does not fix the letter 4, hence we may assume $\varsigma = (432)$, and then $\psi_3\varsigma = (1432)$ has order 4, hence

$$2 = (\text{tr}(\psi_3\varsigma))^2 = (s - s^{-1})^2 a^2 = -3a^2.$$

On the other hand, when $n = 3$ and $3a^2 = -2$, one has $|\psi_3\varsigma| = 4$, so $\langle\psi_1, \varsigma\rangle$ is a quotient of S_4 . Thus $\#\Gamma \leq 24$.

- (ii) If $n = 4$, then we may assume $\varsigma = (4321)$, so $\psi_2 = (34)$ commutes with ψ_4 . This implies $(s^4 - 1)ab = 0$ which is absurd.

(d) If $\Gamma \leq A_5$ and $\Gamma \not\leq A_4$, then $\Gamma = A_5$ by (a) and Proposition 2.4 (d). Arguing similarly as in (c), we can show $\varsigma \in \Gamma$. By Theorem 4.1, (up to isomorphism) there are three possibilities.

- (i) $n = 3$ (so that $s^4 + s^2 + 1 = 0$), $\varsigma = (123)$, $\psi_3 = (24)(35)$. Then $\psi_3\varsigma = (12435)$, hence

$$((s - s^{-1})^2 a^2 - 1)^2 = (s - s^{-1})^2 a^2,$$

implying $9a^4 + 9a^2 + 1 = 0$.

Conversely, if $n = 3$ and $9a^4 + 9a^2 + 1 = 0$, then $|\psi_3\varsigma| = 5$, hence $\langle\psi_3, \varsigma\rangle = A_5$, and $\Gamma \leq A_5$.

- (ii) $n = 5$, (so that $s^4 + s^2 + s^{-2} + s^{-4} = -1$), $\varsigma = (12345)$, $\psi_5 = (12)(34)$. Then $\psi_5\varsigma = (135)$, hence

$$1 = (\text{tr}(\psi_5\varsigma))^2 = (s - s^{-1})^2 a^2, \quad (15)$$

Conversely, if $n = 5$ and Eq.(15) holds, then $|\psi_5\varsigma| = 3$, $\langle\psi_5, \varsigma\rangle = \langle\psi_5, \psi_5\varsigma\rangle = A_5$, and $\Gamma \leq A_5$.

- (iii) $n = 5$, $\varsigma = (12345)$, $\psi_5 = (13)(24)$. Then $\psi_5\varsigma^2 = (152)$, hence

$$1 = (\text{tr}(\psi_5\varsigma^2))^2 = (s^2 - s^{-2})^2 a^2, \quad (16)$$

Conversely, when $n = 5$ and Eq.(16) holds, then $|\psi_5\varsigma| = 3$, $\langle\psi_5, \varsigma\rangle = \langle\psi_5, \psi_5\varsigma^2\rangle = A_5$, and $\Gamma \leq A_5$.

Note that $(s - s^{-1})^2 + (s^2 - s^{-2})^2 = -5$ and $(s - s^{-1})^2 \cdot (s^2 - s^{-2})^2 = 5$, hence Eq.(15) or Eq.(16) holds if and only if $1/a^2$ is a root of $t^2 + 5t + 5 = 0$. \square

If $\sigma = \alpha^k$, then $n \mid p - 1$ and $k = (p - 1)u/n$ for some u with $(u, n) = 1$, $1 \leq u < n/2$. Now $\varphi := \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ commutes with α^k and

$$\varphi\omega\varphi^{-1} = \begin{pmatrix} a & 1 \\ -a^2 - 1 & -a \end{pmatrix} =: \omega(\text{ii}, a), \quad (17)$$

hence $\mathcal{CM}_\omega^\sigma \cong \mathcal{CM}_{\omega(\text{ii},a)}^{\alpha^k}$. Furthermore, for $a \neq a'$, there does not exist ϑ with $\vartheta\alpha^k\vartheta^{-1} = \alpha^k$ and $\vartheta\omega(\text{ii},a)\vartheta^{-1} = \omega(\text{ii},a')$, so $\mathcal{CM}_{\omega(\text{ii},a)}^{\alpha^k} \not\cong \mathcal{CM}_{\omega(\text{ii},a')}^{\alpha^k}$.

If $\sigma = \gamma^\ell$, then $n \mid p+1$ and $\ell = (p+1)v/n$ for some v with $(v,n) = 1$, $1 \leq v < n/2$. One deduces from Eq.(2), (10) and (13) that

$$y + ez = -2\check{a}, \quad \text{with } \check{a} = a\sqrt{e} \in \mathbb{F}_p, \quad (18)$$

and then from $x^2 + yz = -1$ that

$$(y + \check{a})^2 - ex^2 = \check{a}^2 + e. \quad (19)$$

The condition $bc \neq 0$ is equivalent to $\check{a}^2 + e \neq 0$. When \check{a} is fixed, the equation (19) has $p+1$ solutions

Choose a solution $(x_{\text{ii},\check{a}}, y_{\text{ii},\check{a}})$, and let

$$\tilde{\omega}(\text{ii}, \check{a}) = \begin{pmatrix} x_{\text{ii},\check{a}} & y_{\text{ii},\check{a}} \\ -(2\check{a} + y_{\text{ii},\check{a}})/e & -x_{\text{ii},\check{a}} \end{pmatrix}. \quad (20)$$

Arguing similarly as in Section 3, we can show that $\mathcal{CM}_\omega^{\gamma^\ell} \cong \mathcal{CM}_{\tilde{\omega}(\text{ii},\check{a})}^{\gamma^\ell}$.

Theorem 4.4. *Suppose \mathcal{M} is an n -valent II-RBCM on $\text{PSL}(2, p)$ with $p > 5$, then $n \mid p(p^2 - 1)$.*

(i) *If $n = p$, then $\mathcal{M} \cong \mathcal{CM}_{\varpi(z)}^\beta$ for a unique $z \neq 0$.*

(ii) *If $n \mid p-1$, then $\mathcal{M} \cong \mathcal{CM}_{\omega(\text{ii},a)}^{\alpha^{(p-1)u/n}}$ for a unique pair (a, u) such that*

- $a \neq 0$ and $a^2 \neq -1$;
- $(u, n) = 1$ and $1 \leq u < n/2$;
- $3a^2 \neq -1, -2$ and $9a^4 + 9a^2 + 1 \neq 0$ if $n = 3$;
- $5a^4 + 5a^2 + 1 \neq 0$ if $n = 5$.

(iii) *If $n \mid p+1$, then $\mathcal{M} \cong \mathcal{CM}_{\tilde{\omega}(\text{ii},\check{a})}^{\gamma^{(p+1)v/n}}$ for a unique pair (\check{a}, v) such that*

- $\check{a} \neq 0$ and $\check{a}^2 \neq -e$;
- $(v, n) = 1$ and $1 \leq v < n/2$;
- $3\check{a}^2 \neq -e, -2e$ and $9\check{a}^4 + 9\check{a}^2e + e^2 \neq 0$ if $n = 3$;
- $5\check{a}^4 + 5\check{a}e + e^2 \neq 0$ if $n = 5$.

Acknowledgements:

I shall express my gratitude to Fangli Zhang for helpful suggestions on simplifying the proves of Lemma 3.2 and 4.3.

References

- [1] M. Artin, *Algebra*. China Machine Press, Beijing, 2004.
- [2] H.M. Chen, *A new approach to regular balanced Cayley maps on abelian groups*. arXiv:1407.5295.
- [3] L.E. Dickson, *Linear groups: with an exposition of the Galois field theory*. Dover Publications, New York, 1902.
- [4] W. Fulton, J. Harris, *Representation theory: a first course*. Springer-Verlag, 1950.
- [5] Y. Fuertes, G. Jones, *Beauville surfaces and finite groups*. J. Algebra 340 (2011), no. 1, 13–27.
- [6] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics, vol. 84, 2nd edition, Springer-Verlag, New York, 1990.
- [7] J.H. Kwak, J. Oh, *A classification of regular t -balanced Cayley maps on dicyclic groups*. European J. Combin. 29 (2008), no. 5, 1151–1159.
- [8] P. Morandi, *Field and Galois theory*. Graduate Texts in Mathematics, vol. 167, Springer-Verlag, New York, Berlin, Heidelberg, 1996.
- [9] J. Oh, *Regular t -balanced Cayley maps on semi-dihedral groups*. J. Combin. Theory Ser. B 99 (2009), no. 2, 480–493.
- [10] R.B. Richter, J. Širáň, R. Jajcay, T.W. Tucker, M.E. Watkins, *Cayley maps*. J. Combin. Theory, Ser. B 95 (2005), 189–245.
- [11] M. Škoviera, J. Širáň, *Regular maps from Cayley graphs, Part 1: balanced Cayley maps*. Discrete Math. 109 (1992), 265–276.
- [12] Y. Wang, R. Feng, *Regular balanced Cayley maps for cyclic, dihedral and generalized quaternion groups*. Acta Math. Sin. (Engl. Ser.) 21(2005), no. 4, 773–778.